KOREAN PATENT ABSTRACTS(KR)

Document Code: A
(11) Publication No. 1020000029343 (43) Publication.Date. 20000525
(21) Application No. 1019990046783 (22) Application Date. 19991027
(51) IPC Code:
H04L 9/32

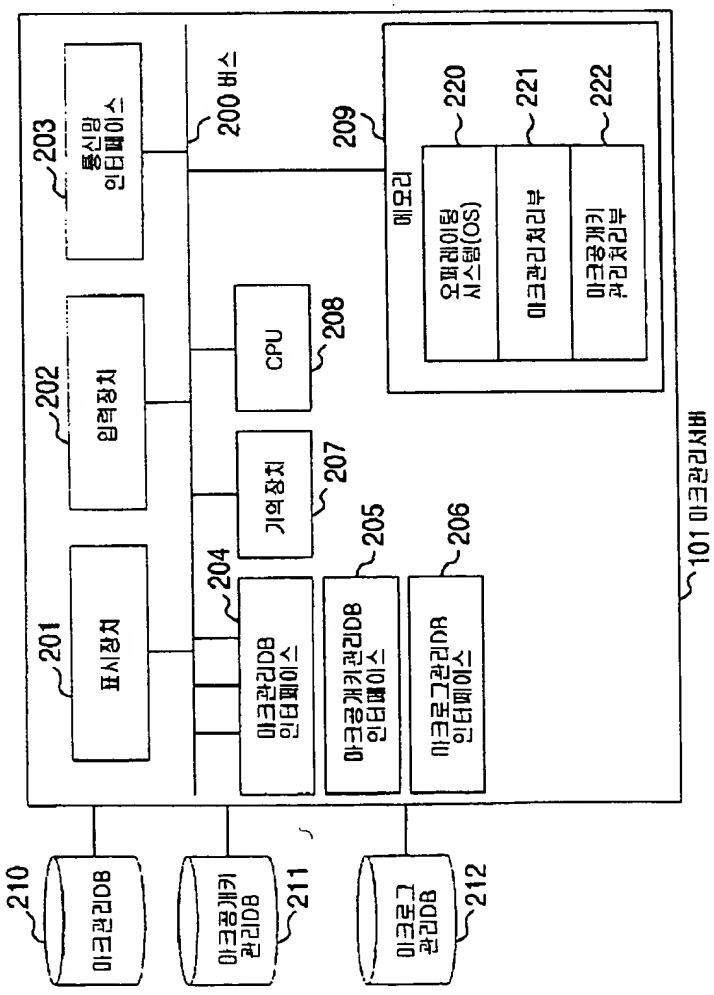
(71) Applicant:
HITACHI LTD.
(72) Inventor:
NAGAI YASHIKO
TOYOSHIMA HISASI
TSUCHIYAMA CHIKAKO

(30) Priority:

(54) Title of Invention

METHOD FOR MANAGING AUTHENTICATION MARK, DIGITAL SIGNATURE OR AUTHENTICATION SYSTEM OF ELECTRONIC SEAL

Representative drawing



(57) Abstract:

PURPOSE: A method for managing an authentication mark, a digital signature or an authentication system of electronic sea is provided to realize a person authentication or data authentication when transmitting and receiving digital data on a network.

CONSTITUTION: A mark management server(101) performs the authentication of digital data by a digital mark. The server comprises a mark management processing unit (221) which receives a mark registration request requesting a new registration or update of a mark from a mark terminal apparatus. And also the mark management processing unit makes out a mark by inputting a person authentication information encoding the information to authenticate a person of a requester with an encode key in a mark design of the concerned requester, and distributes the mark to the requester by attaching a decode key to decode the person authentication information. The server also comprises a mark decode key management processing unit(222) which registers the decode key to decode the encoded person authentication information in a decode key

management DB, and transmits the registered decode key to each mark terminal apparatus.

if display of image is failed, press (F5)

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51)◦Int. Cl. [6]
H04L 9 /32

(11) 공개번호 특2000-0029343
(43) 공개일자 2000년05월25일

(21) 출원번호 10-1999-0046783
(22) 출원일자 1999년10월27일
(30) 우선권주장 98-309806 1998년10월30일 일본(JP)
(71) 출원인 가부시키가이샤 히타치세이사쿠쇼 가나이 쓰토무
일본 도쿄토 치요다쿠 간다스루가다이 4쪼메 6반치
(72) 발명자 쯔치야마치카코
일본국도쿄도분쿄쿠코이시카와2쵸메6-5-402
토요시마히사시
일본국하치오지시오쯔카1709-19
나가이야스히코
일본국분쿄쿠혼고4쵸메13-12-202
(74) 대리인 이종일
심사청구 : 있음

(54) 디지털서명 혹은 전자인감 인증시스템, 인증마크 관리방법

요약

본 발명은 디지털서명 혹은 전자인감 인증시스템 및 인증마크관리 프로그램에 관한 것으로, 디지털마크에 의해 디지털데이터의 인증을 수행하는 마크관리서버에 있어서, 상기 서버는 마크의 신규등록 또는 갱신을 요구하는 마크등록요구를 마크단말장치로부터 수신하고, 요구자의 인물을 인증하기 위한 정보를 암호키로 암호화한 본인인증정보를 당해 요구자의 마크디자인에 집어넣어 마크를 작성하고, 상기 작성한 마크에 상기 본인인증정보를 복호(復號)화하기 위한 복호키를 첨부하여 요구자에게 배포하는 마크관리처리부와, 상기 암호화한 본인인증정보를 복호화하기 위한 복호키를 마크복호키 관리DB에 등록하고, 상기 등록한 복호키를 각 마크단말장치에 송신하는 마크복호키 관리처리부를 갖춤으로써, 네트워크상에서 디지털데이터를 송수신할 때의 본인인증 및 데이터인증을 실현할 수 있는 기술이 제시된다.

대표도

도1

명세서

도면의 간단한 설명

도 1은 본 실시예의 전자인감 인증시스템의 개략구성을 나타내는 도이다.

도 2는 본 실시예의 인감마크 관리서버(101)의 개략구성을 나타내는 도이다.

도 3은 본 실시예의 사원단말(111)의 개략구성을 나타내는 도이다.

도 4는 본 실시예의 인감마크 관리DB(210)의 데이터예를 나타내는 도이다.

도 5는 본 실시예의 인감마크 공개키(key) 관리DB(211)의 데이터예를 나타내는 도이다.

도 6은 본 실시예의 본인인증데이터의 예를 나타내는 도이다.

도 7은 본 실시예의 문서인증데이터의 예를 나타내는 도이다.

도 8은 본 실시예의 인영 및 인감마크의 이미지예를 나타내는 도이다.

도 9는 본 실시예의 초기화면의 이미지예를 나타내는 도이다.

도 10은 본 실시예의 인감마크 등록처리의 처리절차를 나타내는 순서도이다.

도 11은 본 실시예의 인감마크 날인처리의 처리절차를 나타내는 순서도이다.

도 12는 본 실시예의 도 11의 처리순서에 대응하는 처리화면의 이미지를 나타내는 도이다.

도 13은 본 실시예의 본인인증처리의 처리절차를 나타내는 순서도이다.

도 14는 본 실시예의 도 13의 처리순서에 대응하는 처리화면의 이미지를 나타내는 도이다.

도 15는 본 실시예의 문서인증처리의 처리절차를 나타내는 순서도이다.

도 16은 본 실시예의 도 15의 처리순서에 대응하는 처리화면의 이미지를 나타내는 도이다.

< 도면의 주요부분에 대한 부호의 설명 >

108 : 인터넷　　501 : 데이터번호

801~803 : 인영이미지

1201~1203, 1401~1403, 1601, 1602 : 처리화면이미지

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 디지털데이터를 전자적인 마크를 통해 인증하는 디지털마크 인증시스템에 관한 것으로, 특히 디지털데이터를 인영, 혹은 서명을 나타내는 디지털마크를 통해 인증하는 디지털마크 인증시스템에 적용하여 유효한 기술에 관한 것이다.

네트워크상에서의 상거래 등이 확산되고 있는 오늘날에는, 전달하는 정보의 확실성을 네트워크상에서 확인할 수 있는 기술이 중요시되어 오고 있다. 제 3자가 본인임을 가장하고 있는 것은 아닌지를 확인하는 본인인증에 대해서는, 여권이나 신용카드 등 소유물을 이용하는 방식, 지문, 목소리나 필적 등의 바이오메트릭스를 이용하는 방식, 비밀번호나 디지털서명 등의 비밀정보를 이용하는 방식 등이 있는데, 네트워크에서 이용하는 경우에는 소유물이나 비밀정보를 이용하는 방식이 일반적이다.

또한, 정보를 전달하는 과정에서의 도중 개찬(改竄)에 대한 확인은, 인터넷을 이용한 EC(Electronic Commerce)에 있어서, 신용결제를 안전하게 수행하기 위해 이용되는 SET(Secure Electronic Transactions)에서는 디지털서명을 통한 카드소유자의 인증을 실시하고 있다. 디지털서명은 통상 전달하고자 하는 정보, 즉 메세지를 압축한 압축문을 송신인의 암호키로 암호화한 암호문이며, 송신인의 복호(復號)키(key)(공개키)로 처음의 압축문으로 복호할 수 있다. 즉, 수신인은 받은 메세지로 만든 압축문과 받은 디지털서명으로 복호시킨 압축문을 비교함으로써 메세지가 개찬되어 있는지의 여부를 확인, 즉 문서인증을 할 수 있다.

발명이 이루고자하는 기술적 과제

그러나, 문서 등의 디지털데이터의 수신인은 그 디지털데이터를 보는 것만으로는 정보의 정당성이나 송신인의 확인을 할 수 없다. 현실 사회에서는 종이 위에 날인된 도장처럼 직접 눈으로 보고 확인할 수 있는 것에만 안심을 할 수 있는데, 디지털서명은 이와 같이 안심할 수 있는 시인성(視認性)을 갖지 못하고 있다.

한편, 종래의 전자인감 시스템에서는 눈으로 보고 확인할 수 있는 인영을 이용하는데, 인영자체는 단순한 디자인으로, 문서 등의 디지털데이터의 수신인이 송신인을 확인하기에는 로그정보 등의 이력을 조사할 필요가 있었다.

본 발명의 목적은, 상기 문제를 해결하여 네트워크상에서 디지털데이터를 송신 및 수신할 때의 본인인증 또는 데이터인증을 실현할 수 있는 기술을 제공하는 데에 있다.

또한, 본 발명의 다른 목적은, 눈으로 직접 확인할 수 있는 마크를 포함하는 송신메세지의 인증이 가능한 기술을 제공하는 데에 있다.

본 발명에 의하면, 디지털마크에 의해 데이터를 인증하기 위한 마크를 제공하기 위한 디지털마크 인증시스템으로서, 마크를 작성하기 위한 요구에 따라서, 디스플레이상에서 시인성이 있는 마크를 작성하기 위해 요구자의 마크디자인에 요구자의 인증정보를 집어넣는 마크관리처리부(221)와, 상기 마크를 복호시키기 위한 복호키와 상기 시인성마크를 요구자 단말장치에 배포하는 마크배포부(200-222)를 가지는 상기 시스템이 제공된다.

이 작성된 마크 안에 인증정보가 들어가 있다는 것을 디스플레이상에서 눈으로 직접 확인할 수 있다. 인증정보는 요구자의 특징을 포함하는 정보를 암호키로 암호화함으로써 얻을 수 있다.

또한, 이 마크갱신요구에 따라, 상기 마크관리처리부(221)는 요구자의 다른 인증정보를 작성하기 위하여 요구자의 다른 특징을 포함하는 정보를 암호키로 암호화하고, 상기 마크를 작성하기 위해 요구자의 마크디자인에 상기 다른 인증정보를 집어넣을 수가 있다.

또한, 디지털마크에 의해 데이터를 인증하기 위한 마크를 디지털데이터에 부가하는 단말장치로서,

마크를 작성하기 위한 요구를 디지털마크 인증시스템에 송신하고, 그 시스템으로부터 요구자 본인의 특징을 포함하는 정보를 암호키로 암호화하여 요구자의 마크디자인에 상기 인증정보를 집어넣은 마크를 수신하여 기억하는 마크처리부(312)와, 상기 마크를 복호하기 위한 복호키를 수신하여 격납하기 위한 복호키 데이터베이스(315)와, 송신될 디지털데이터를

인증하기 위해 상기 디지털데이터의 로그정보를 상기 암호키로 암호화하여 상기 마크에 집어넣어 상기 디지털데이터와 함께 송신하는 송신부(303)를 가지는 상기 단말장치가 제공된다.

또한, 본 발명에 의하면, 디지털마크에 의해 데이터를 인증하기 위한 인증시스템으로서, 마크를 작성하기 위한 요구에 따라서, 디스플레이상에서 시인성이 있는 마크를 작성하기 위해 요구자의 마크디자인에 요구자의 인증정보를 집어넣는 마크관리처리부(221)와, 상기 마크를 복호하기 위한 복호키와 상기 시인성마크를 부여하는 마크관리부(200-222)와, 송신될 디지털데이터를 인증하기 위해 상기 디지털데이터의 로그정보를 상기 암호키로 암호화하여 상기 마크에 집어넣어 상기 디지털데이터와 함께 송신하는 송신부(303)를 가지는 인증시스템이 제공된다.

또한, 인영 또는 서명을 나타내는 마크에 의해 디지털데이터의 인증을 실시하는 전자마크 인증시스템의 마크인증처리부에 있어서, 마크디자인에 본인인증정보 및 디지털데이터 인증정보를 집어넣은 마크를 디지털데이터에 부가하여 마크안의 인증정보를 이용하여 당해 디지털데이터의 인증을 실시할 수 있다.

본 발명의 마크단말장치의 마크등록처리부가 전자인감 등의 마크의 신규등록 또는 갱신을 요구하는 마크등록요구를 마크관리서버에 송신하면, 마크관리서버의 마크관리처리부는 마크등록요구를 수신하여 요구자의 인물을 인증하기 위한 정보를 암호키로 암호화한 본인인증정보를 당해 요구자의 인영디자인 등의 마크디자인에 집어넣어 마크를 작성하고, 상기 작성한 마크에 상기 본인인증정보를 복호하기 위한 복호키를 첨부하여 요구자에게 배포한다.

또한, 마크관리서버의 마크복호키 관리처리부는, 상기 암호화한 본인인증정보를 복호하기 위한 복호키를 마크복호키 관리DB에 등록하고, 상기 등록한 복호키를 각 마크단말장치에 송신한다.

마크단말장치의 마크등록처리부는, 마크관리서버의 마크관리처리부에서 송신된 마크를 건네받고, 또한 각 마크단말장치의 복호키 격납처리부는 마크복호키 관리처리부에서 송신된 복호키를 수신하여 복호키 DB에 격납한다.

마크단말장치의 마크부가처리부는, 마크가 부가되는 문서 등의 디지털데이터에 대하여 그 특징정보를 포함하는 디지털데이터 인증정보와 마크부가 통산번호를 사용자 고유의 암호키로 암호화하고, 당해 디지털데이터를 송신하는 사용자의 본인인증정보가 들어간 마크에 상기 암호화된 디지털데이터 인증정보 및 마크부가 통산번호를 집어넣어 상기 디지털데이터의 선택된 위치에 상기 마크를 부가한다.

상기와 같이 마크가 부가된 디지털데이터가 다른 사용자의 마크단말장치에 송신되면, 그 마크단말장치의 마크인증처리부는 디지털데이터에 부가된 마크에서 본인인증정보를 추출하고, 그 본인인증정보를 복호하기 위해 첨부된 복호키가 복호키 DB에 격납되어 있는 복호키와 합치되는 지의 여부를 조회하고, 상기 복호키가 합치하는 경우에는 상기 마크에서 추출한 본인인증정보를 상기 복호키로 복호하여 본인인증정보를 표시하고, 합치하지 않은 경우에는 에러메세지를 표시한다.

또한, 마크단말장치의 마크인증처리부는, 디지털데이터에 부가된 마크에서 디지털데이터 인증정보를 추출하여 복호키를 통해 복호화하고, 마크가 부가되어 있는 디지털데이터에서 특징정보를 추출하여, 상기 디지털데이터에서 추출한 특징정보와 마크에서 추출한 디지털데이터 인증정보 중의 특징정보를 비교조회하여, 특징정보가 합치하는 경우에는 상기 디지털데이터 인증정보의 표시를 실시하고, 합치하지 않는 경우에는 에러메세지를 표시한다.

이상과 같이 본 발명의 전자마크 인증시스템에 의하면, 본인인증정보 및 디지털데이터 인증정보를 집어넣어 작성한 마크를 디지털데이터에 부가하여, 마크안의 인증정보를 이용하여 당해 디지털데이터의 인증을 실시하기 때문에, 네트워크상에서 디지털데이터를 송수신할 때의 본인인증 및 데이터인증을, 데이터의 송신인을 상징하는 것에 의한 시인성을 확인한 후 실현할 수 있다.

발명의 구성 및 작용

이하, 기업내부 네트워크 및 기업간 네트워크에 있어서, 디지털서명 또는 인감을 이용하여 본인인증 및 문서인증을 실시하는 한 실시예의 전자마크 인증시스템에 대하여 설명하기로 한다.

도 1은 실시예의 디지털마크 인증시스템의 개략구성을 나타내는 도이다. 본 실시예의 전자마크 인증시스템은, 인감마크 또는 서명마크를 관리하는 복수의 시스템관리자(100A~100B)(이하, 간단하게 시스템관리자(100)라 부른다)와 복수의 사원(110A~110B)(이하, 간단하게 사원(110)이라 부른다)이 이용하는 시스템으로서, 도 1에 나타낸 바와 같이 마크관리서버(101A)(이하, 간단하게 마크관리서버 (101)라 부른다)와 사원단말(111A)(이하, 간단하게 사원단말(111)이라 부른다)이 기업내부 네트워크 등의 통신망(120A)(이하, 간단하게 통신망(120)이라 부른다)을 매개로 서로 접속되어 구성되어 있다. 이에 인터넷(108) 등을 경유하여 BB사의 동일 시스템 혹은 클라이언트단말이 접속된다.

또한, 여기서 말하는 마크란, 사인성이 있는 본인의 상징성을 나타내는 요소를 가지는 화상데이터로서, 제 3자가 인감을 날인하거나 혹은 서명을 사인하는 본인으로 위장하고 있지는 않는지에 대한 검증(이하, 간단하게 본인인증이라 부른다) 및 날인 또는 사인된 문서 등의 디지털데이터가 개찬되어 있지는 않는지에 대한 검증(이하, 간단하게 문서인증이라 부른다)을 실시하기 위한 이미지디자인의 형상을 취하는 인감이나 사인마크를 나타내는 것으로 한다. 이 이미지디자인은 활자의 코드화정보보다 장황해도 된다.

마크관리서버(101)는, 시스템관리자(100)가 관리하는 기업내부 네트워크나 기업간의 네트워크 거래에서 본인인증이나 문서인증을 실시한다. 마크관리서버 (101)는 사원(110)의 요구에 따라서 각자의 본인인증에 필요한 정보로서 마크를 후술할 마크관리 DB에 등록한다. 이 때, 마크의 디자인은 스캐너로 실제의 인영, 사인, 얼굴사진 등을 디지털화하는 등의 방법으로 사원(110)이 자유롭게 작성할 수 있는데, 부정한 등록을 방지하기 위해 사원ID 등으로 이 작성자의 확인을 실시한다.

사원(110)은 사원단말(111)을 사용하여 비지니스에 필요한 문서 등을 작성하거나, 시스템관리자(100)와 데이터의 송수신을 한다. 각자의 마크는 사원단말(111) 등에서 관리된다. 소속 등의 인감 또는 서명에 포함되는 정보변경을 작성자가 요구하였을 때에는, 시스템관리자(100)가 마크의 갱신을 실시하여 갱신된 마크를 사원단말(111)에 송신한다. 화면이미지(112)는 인감마크첨가 디지털데이터를 표시하였을 때의 화면표시예이다.

도 2는 본 실시예의 마크관리서버(101)의 개략구성을 나타내는 도이다. 도 2에 나타낸 바와 같이 본 실시예의 마크관리서버(101)는 마크관리처리부(221)와 마크공개키 관리처리부(222)를 가지고 있다.

마크관리처리부(221)는 마크의 신규등록 또는 갱신을 요구하는 마크등록요구를 통신망(120A)을 매개로 사원단말(111)에서 수신하고, 요구자의 인물을 인증하기 위한 정보를 비밀키로 암호화한 본인인증정보를, 후술할 전자음화(陰畵)기술로 당해 요구자의 인영 혹은 서명디자인에 집어넣어 마크를 작성하고, 상기 작성한 마크에 상기 본인인증정보를 복호하기 위한 공개키를 첨부하여 요구자에게 배포하는 마크관리처리부이다.

마크공개키 관리처리부(222)는, 암호화한 본인인증정보를 복호하기 위한 공개키를 마크공개키 관리 DB(211)에 등록하고, 상기 등록한 공개키를 각 사원단말(111)에 송신하는 마크공개 혹은 복호키 관리처리부이다.

마크관리서버(101)를 마크관리처리부(221) 및 마크공개키 관리처리부(222)로서 기능시키기 위한 프로그램은, CD-ROM 등의 기록매체에 기록되어 자기디스크 등에 격납된 후, 메모리에 로드되어 실행되는 것으로 한다. 또한, 상기 프로그램을 기록하는 매체는 CD-ROM 이외의 다른 매체를 사용할 수도 있다.

도 2에 나타낸 바와 같이, 본 실시예의 마크관리서버(101)는, 표시장치(201)와, 입력장치(202)와, 통신망 인터페이스(203)와, 마크관리DB 인터페이스(204)와, 마크공개키관리DB 인터페이스(205)와, 마크로그관리DB 인터페이스(206)와, 기억장치(207)와, CPU(208)와, 메모리(209)가 버스(200)에 의해 서로 접속되어 구성되어 있다. 또한, 외부기억장치로서 마크관리DB(210), 마크공개키관리DB(211) 및 마크로그관리DB(212)가 접속되어 있다.

표시장치(201)는, 마크관리서버(101)를 사용하는 시스템관리자(100)에게 메세지 등을 표시하기 위해 이용되는 것으로, CRT나 액정디스플레이 등으로 구성된다. 입력장치(202)는 마크관리서버(101)를 사용하는 시스템관리자(100)가 데이터나 명령 등을 입력하기 위해 이용되는 것으로, 키보드와 마우스 등으로 구성된다. 통신망 인터페이스(203)는 통신망(120)을 매개로 사원단말(111)이나 타사의 마크관리서버 (101B) 등과 데이터의 송수신을 실시하기 위한 인터페이스이다.

마크관리DB 인터페이스(204)는, 마크관리DB(210)와 데이터의 송수신을 실시하기 위한 인터페이스이다. 마크관리DB(210)는

사원ID, 인감/서명ID, 인감/서명 등과 같은 데이터를 대응시켜 관리하는 것으로, 예를들어 도 4와 같은 것이다.

마크공개키관리DB 인터페이스(205)는, 마크공개키관리DB(211)와 데이터의 송수신을 실시하게 위한 인터페이스이다. 마크공개키관리DB(211)는 거래가 있는 기업의 정보시스템 관리부처 등의 마크관리자와 본인인증용 공개키 등과 같은 데이터를 대응시켜 관리하는 것으로, 예를들면 도 5와 같은 것이다.

마크로그관리DB 인터페이스(206)는, 마크로그관리DB(212)와 데이터의 송수신을 실시하기 위한 인터페이스이다. 마크로그관리DB(212)는 사원단말(111)에서 디지털데이터에 마크를 날인/서명할 때에 그 마크에 집어넣는 문서인증데이터를 대응시켜 관리하는 것으로, 예를들면 도 7과 같은 것이다.

기억장치(207)는, 마크관리서버(101) 등에서 사용되는 프로그램과 데이터를 영속적으로 기억하기 위해 이용되는 것으로, 하드디스크와 플로피디스크 등으로 구성된다.

CPU(208)는, 마크관리서버(101)를 구성하는 각부를 통괄적으로 제어하거나, 여러가지 연산처리를 수행한다. 메모리(209)에는 OS(220)나 마크관리처리부(221), 마크공개키 관리처리부(222)와 같은 CPU(208)가 상기의 처리를 하기 위해 필요한 프로그램 등이 일시적으로 격납된다.

여기서, OS(220)는 인감마크관리서버(101) 전체의 제어를 수행하기 위해 파일관리와 프로세스관리 혹은 디바이스관리와 같은 기능을 실현하기 위한 프로그램이다.

마크관리처리부(221)는, 사원단말(111)로부터 마크등록/변경요구가 있는 경우에, 제 3자로부터의 부정한 요구가 아닌지의 여부를 확인하는 처리, 등록한다고 판단한 경우에 송부된 서명 또는 인영디자인 또는 마크관리DB(210)에서 관리하고 있는 디자인에 본인정보를 집어넣는 처리, 처리에 기초하여 마크관리DB(210)를 갱신하는 처리, 요구자에게 마크를 송신하는 처리 및 마크날인시에 송신되는 로그정보를 마크로그관리DB(212)에 격납하는 처리를 수행하는 처리부이다.

또한, 마크관리DB(210)는, 권한을 가진 자만이 갱신할 수 있는 것으로 한다. 또한, 디자인에 집어넣는 본인정보는 도 6과 같은 것이다. 화상데이터안에 특정한 정보를 집어넣는 기술은 「전자음화(電子陰畵)」로서 알려져 있다. 이에는, 인간의 눈으로는 판별할 수 없도록 정보를 집어넣는 비가시(非可視) 음화와, 인간의 눈으로도 볼 수 있는 형태로 정보를 집어넣는 가시음화가 있으며, 비가시 음화의 경우에는 집어넣는 정보량에 한계가 있다고 하지만, 부정을 방지하기 위해 유효한 경우도 적지않다. 마크이미지가 상징하는 의미를 알 수 있는 범위, 즉 그 마크가 무엇을 나타내는가를 알 수 있는 범위라면 다소 디자인을 변경해도 지장이 없기 때문에, 도 8과 같이 가시음화와 비가시 음화를 조합하여 어느 정도 많은 정보를 집어넣을 수 있다.

마크공개키 관리처리부(222)는, 외부 디지털문서에 날인된 마크의 송신인의 확인, 즉 본인인증을 실시하기 위해 필요한 공개키를 마크공개키관리DB(211)에 등록· 관리하는 처리, 새로운 공개키가 마크공개키관리DB(211)에 등록되면 사원단말(111) 등에 접속되어 있는 공개키DB에 그 공개키를 송신하는 처리, 및 공개키의 송신요구가 있는 경우에는 요구자에게 그 공개키를 송신하는 처리를 수행하는 처리부이다.

또한, 외부로부터 공개키를 받은 경우에는, 제 3자가 기업의 시스템관리자 (100)로 가장하는 것을 방지하기 위하여, 발신자의 신원확인을 실시한 후에 FD 등에 격납시킨 공개키를 받는 것으로 한다.

도 3은 본 실시예의 사원단말(111)의 개략구성을 나타내는 도이다. 도 3에 나타낸 바와 같이, 본 실시예의 사원단말(111)은 마크등록처리부(312)와, 마크날인처리부(313)와, 마크인증처리부(314)와, 공개키격납처리부(315)를 가지고 있다.

마크등록처리부(312)는, 마크의 신규등록 또는 갱신을 요구하는 마크등록요구를 마크관리서버(101)에 송신하고, 요구자의 인물을 인증하기 위한 정보를 비밀키로 암호화한 본인인증정보를 당해 요구자의 디자인에 집어넣어 작성한 마크를 마크관리서버(101)로부터 건네받은 마크등록처리부이다.

마크날인처리부(313)는, 마크가 부가되는 문서의 특징정보를 포함하는 문서인증정보와 통산번호를 사용자 고유의 비밀키

로 암호화하고, 본인인증정보가 들어간 마크에 상기 암호화된 문서인증정보 및 통산번호를 집어넣어, 상기 문서의 선택된 위치에 상기 마크를 부가하는 마크부가처리부이다.

마크인증처리부(314)는, 문서에 부가된 마크에서 본인인증정보를 추출하고, 그 본인인증정보를 복호하기 위해 첨부된 공개키가 공개키DB(309)에 격납되어 있는 공개키와 합치하는 지의 여부를 조회하여, 상기 공개키가 합치하는 경우에는 상기 마크에서 추출한 본인인증정보를 상기 공개키로 복호시켜 본인인증정보를 표시하고, 합치하지 않는 경우에는 에러메세지를 표시하는 본인인증처리와, 문서에 부가된 마크에서 문서인증정보를 추출하여 공개키에 의해 복호하고, 마크가 부가되어 있는 문서에서 특징정보를 추출하여 상기 문서에서 추출한 특정정보와 마크에서 추출한 문서인증정보 내의 특징정보를 비교조합하여, 특징정보가 합치하는 경우에는 상기 문서인증정보의 표시를 실시하고, 합치하지 않는 경우에는 에러메세지를 표시하는 데이터인증처리를 실시하는 마크인증처리부이다. 공개키격납처리부(315)는, 본인인증정보를 복호하기 위한 공개키를 마크관리서버(101)로부터 수신하여, 상기 공개키를 공개키DB(309)에 격납하는 복호키격납처리부이다.

사원단말(111)을 마크등록처리부(312), 마크날인처리부(313), 마크인증처리부(314) 및 공개키격납처리부(315)로서 기능시키기 위한 프로그램은, CD-ROM 등의기록매체에 기록되어 자기디스크 등에 격납된 후, 메모리에 로드되어 실행되는 것으로 한다. 또한, 상기 프로그램을 기록하는 매체는 CD-ROM 이외의 다른 매체를 사용할 수 있다.

도 3에 나타낸 바와 같이, 본 실시예의 사원단말(111)은 표시장치(301)와, 입력장치(302)와, 통신망 인터페이스(303)와, 공개키DB 인터페이스(304)와, 기억장치(305)와, CPU(306)와, 메모리(307)가 버스(300)에 의해 서로 접속되어 구성되어 있다. 종래 실제 사회에서 사용하고 있는 디자인을 이용하는 경우에는, 이미지스캐너(308)를 접속하여 사용하고자 하는 디자인을 비트맵 등으로 읽은 후에 편집할 수 있도록 한다.

표시장치(301)는, 사원단말(111)을 사용하는 사원(110)에 메세지 등을 표시하기 위해 이용되는 것으로, CRT와 액정디스플레이 등으로 구성되어 있다. 입력장치(302)는, 사원단말(111)을 사용하는 사원(110)이 데이터나 명령 등을 입력하기 위해 이용되는 것으로, 키보드와 마우스 등으로 구성된다. 통신망 인터페이스(303)는, 통신망(120)을 매개로 마크관리서버(101)나 사원단말(111B) 등과 데이터의 송수신을 수행하기 위한 인터페이스이다.

공개키DB 인터페이스(304)는, 공개키DB(309)가 있는 경우에 데이터의 송수신을 수행하기 위한 인터페이스이다. 기억장치(305)는, 사원단말(111) 등에서 사용되는 프로그램이나 데이터를 영속적으로 기억하기 위해 이용되는 것으로, 하드디스크와 플로피디스크 등으로 구성된다.

CPU(306)는, 사원단말(111)을 구성하는 각부를 통괄적으로 제어하거나, 여러가지 연산처리를 실시한다. 메모리(307)에는 OS(310)와 그룹웨어시스템(311) 등, 마크인증처리부(314), 마크정보기억부(316)와 같은 CPU(306)가 상기의 처리를 하기 위해 필요한 프로그램 등이 일시적으로 격납된다.

여기서, OS(310)는 사원단말(111) 전체의 제어를 수행하기 위해 파일관리와 프로세스관리 혹은 디바이스관리와 같은 기능을 실현하기 위한 프로그램이다. 그룹웨어시스템(311) 등은 사원단말(111)이 사내외와 디지털데이터를 송수신하고, 필요한 데이터를 표시하기 위한 시스템으로, 디지털데이터에 부가된 인증정보를 취급하기 위해 마크인증처리부(314)와의 인터페이스를 가진다. 또한, 이 그룹웨어시스템(311) 등의 부분은, 디지털데이터를 핸들링하는 어플리케이션시스템이라면 어떠한 것이라도 좋으며, 특별히 그룹웨어시스템에 한정되는 것은 아니다. 또한, 직접마크인증처리부(314)를 개별 어플리케이션시스템으로 하여 OS(310)상에서 움직이는 경우도 있다.

마크등록처리부(312)는, 마크등록을 위한 디자인을 작성하는 처리, 마크관리서버(101)에 마크등록요구를 송신하는 처리 및 마크관리서버(101)로부터 송신된 마크를 수신하는 처리를 수행한다.

마크날인처리부(313)는, 사원(110)이 사원단말(111)에서 디지털데이터에 디지털서명 또는 인감을 서명 또는 날인하기 위한 처리로서, 필요한 디지털데이터를 표시하고, 사원ID에 대응하는 비밀번호가 입력되면 그 사원ID에 대응하는 마크를 불러내는 처리, 선택된 문서인증정보와 마크의 날인통산번호 등의 서명/날인시 정보를 고유의 비밀키로 암호화한 것을 마크의 특정 블럭에 집어넣는 처리 및 문서의 지정된 위치에 마크를 날인하는 처리 등을 실시한다.

마크인증처리부(314)는, 사원(110)이 사원단말(111)에서 수신한 디지털데이터의 송신인이나 내용의 인증을 실시하기 위한 처리부이다. 필요한 디지털데이터를 표시하고, 선택된 인증항목에 대응하여 마크에 들어간 본인인증정보를 미리 마크관리서버(101)로부터 배포된 공개키로 복호하여 표시하는 본인인증처리, 마크에 들어간 문서인증정보를 마크에 첨부된 공개키로 복호하여 표시하는 문서인증처리, 상기 공개키로 복호할 수 없는 경우에 에러메세지를 표시하는 처리 및 표시한 디지털데이터의 유효기한과 파일명 등의 정보를 체크하고, 무효로 판단되는 경우에는 상술한 디자인을 무효의 디자인으로 변형시키는 처리 등을 수행한다.

마크정보기억부(316)는, 마크인증처리부(314)에 의해 사원단말(111)에서 불러낸 마크와 공개키를 일시적으로 격납하는 것이다.

또한, 기업간에서 네트워크거래를 실시하는 등, 본인인증정보의 확인을 위해 복수공개키가 필요한 경우에는, 공개키DB(309)를 사원단말(111) 혹은 통신망(120)에 접속하고, 마크공개키관리DB(211)로부터 필요한 공개키를 공개키DB 인터페이스(304)에 송신하여 사원단말(111)에서 참조할 수 있도록 한다. 또한, 기업내부 네트워크 내에서만 마크를 이용하는 경우는, 미리 사원단말(111)에 공개키를 부여해도 되며, 공개키의 격납방법은 한정되어 있지 않다.

도 4는 본 실시예의 마크관리DB(210)의 데이터예를 나타내는 도이다. 사원ID(401), ID(402), 성명(403), 메일주소(404), 소속· 직책 기타 정보(405), 인영데이터(406) 등을 일정한 표기기준을 바탕으로 표기를 통일하여 격납한다. 새로운 마크를 등록하거나, 기존 마크의 소속· 직책 기타정보(405)를 변경하였을 때 등에 마크관리DB(210)를 갱신한다.

도 5는 본 실시예의 마크공개키관리DB(211)의 데이터예를 나타내는 도이다. 데이터번호(501), 마크관리자(502), 관리자주소(503), 공개키데이터(504) 등을 일정한 표기기준을 바탕으로 표기를 통일하여 격납한다. 마크공개키관리DB(211)는, 본인인증을 위한 공개키데이터(504)를 관리하는 DB이며, 새롭게 마크를 이용하는 기업이 늘어나거나, 공개키데이터(504)의 갱신이 있었을 때 등에 마크공개키관리DB (211)를 갱신한다. 또한, 미리 공개키데이터(504)의 유효기한 등이 설정되어 있는 경우는 그 데이터도 관리한다.

도 6은 본 실시예의 본인인증데이터의 예를 나타내는 도이다. 도 6에서는 마크관리서버(101)에 있어서 마크관리처리부(221)가 사원(110)의 요구에 따라 인영에 본인인증정보를 집어넣을 때의 본인인증데이터의 예를 나타내고 있다.

ID(601), 성명(602), 메일주소(603), 소속· 직책 기타(604) 등을 마크관리서버(101)의 마크관리처리부(221)에 의해 마크관리서버(101)에서 관리하는 비밀키로 암호화하여 마크의 실재물로서 집어넣는다. 집어넣을 때에는, 예를들어 도 8의 인영이미지(802)와 같이 인영의 성명부분에 비가시 음화로 집어넣고, 가시음화의 형태로 회사명을 집어넣는다. 즉, 미리 인영을 2개 이상의 블럭으로 구분하여 특정 블럭에 본인인증정보를 집어넣는다. 또한, 사인(社印)과 같은 인감에 있어서는, 서명/날인의 책임부서를 본인인증정보로서 이용하는 경우도 있다.

도 7은 본 실시예의 문서인증데이터의 예를 나타내는 도이다. 도 7에서는 사원단말(111)에 있어서 사원(110)이 디지털데이터에 마크를 날인할 때 문서인증정보로서 들어가는 문서인증데이터의 예를 나타내고 있다.

사원단말(111)의 마크처리부(313)는, ID(701), 마크날인통산번호(702), 작성일시(703), 유효기한(704), 파일명(705), 단말ID(706), 날인하고자 하는 디지털데이터의 특징정보(707) 등을 마크날인처리부(313)가 관리하는 비밀키에 의해 사원단말(111)에서 암호화하여 마크의 실재물로서 집어넣는다. 예를들어, 도 8의 인영이미지(803)와 같이, 본인인증정보를 집어넣는 블럭 이외의 인영의 주변부분에 문서인증정보를 집어넣는다.

디지털데이터의 특징정보(707)로는, 문자데이터의 코드를 수치로 간주하여 가산한, 이른바 체크섬(check sum)이라 불리는 것이나 디지털데이터의 내용의 압축문 등을 이용한다.

또한, 도 7은 마크로그관리DB(212)의 데이터예이기도 하다. 사원단말(111)의 마크날인처리부(313)에 의해서, 도 7과 같은 데이터를 서명/날인할 때의 로그정보로서 마크관리서버(101)에 송신하고, 인감마크관리처리부(221)에 의해 그 로그정보를 마크로그관리DB(212)에 격납한다.

또한, 본인인증 및 문서인증에 필요한 데이터는, 도 6 및 도 7의 예에 한하지 않고, ISO9001의 인증을 취득할 때의 전자데이터의 기록정보로서 필요한 정보를 충족시키는 것으로 한다.

도 8은, 본 실시예의 인영 및 마크의 이미지예를 나타내는 도이다. 예를들어, 인영이미지(801)와 같은 인영에 본인인증정보를 집어넣는다. 이 때, 미리 인영을 2개 이상의 블럭으로 구분하여 각각 특정 블럭에 본인인증정보와 문서인증정보를 집어넣기로 한다.

예를들어, 인영이미지(802)와 같이 성명부분과 가시음화의 회사명 부분에 본인인증정보를 집어넣고, 인영이미지(803)와 같은 인영의 주변부분에 문서인증정보를 집어넣는 식의 블럭구분을 실시하여, 사원단말(111)의 마크인증처리부(314)에서 인증정보를 복호할 때에는 대응하는 블럭에서 들어있는 정보가 자동적으로 추출되도록 한다.

또한, 인영이미지(801)에서는, 인영디자인예로서 개인의 막도장 디자인을 이용하였는데, 날짜가 들어간 직인이나 사인 등의 디자인으로 할 수도 있고, 또한 사인(社印)으로 이용할 때에는 기업명 등으로 할 수도 있어, 인영이미지(801)의 인영디자인에에 한정되는 것이 아니다. 단, 단순한 이미지디자인과는 달리 인증정보가 들어가 있다고 느낄 수 있는 신뢰감을 주는 인영디자인이어야 한다는 것이 중요하다.

다음으로, 본 실시예의 전자인증시스템의 동작에 대해서 설명하기로 한다. 도 9는 본 실시예의 초기화면의 이미지예를 나타내는 도이다. 도 9에서는 사원단말(111)에 의해 표시되는 전자인증시스템의 초기화면이미지예를 나타내고 있다.

초기화면(900)은, 필요한 디지털문서 등을 표시하는 디지털데이터 표시영역(901)과, 마크의 기능아이콘이 나열되어 있는 마크기능 표시영역(902), OK, 취소, 파일과 같은 기본기능의 아이콘이 나열되어 있는 기본기능 표시영역(903)에 의해 구성된다. 단, 초기화면(900)은 각 영역의 배치예이며, 이 배치에 한정되는 것은 아니다.

도 10은 본 실시예의 마크등록처리의 처리절차를 나타내는 순서도이다. 도 10에서는 사원단말(111)과 마크관리서버(101) 사이에서 마크의 등록을 실시하는 처리순서를 나타내고 있다.

우선, 사원(110)이 도 9와 같은 초기화면(900)의 마크기능 표시영역(902)의 등록버튼을 클릭하면, 마크등록처리부(312)는 마크의 등록요구를 마크관리서버 (101)에 송신한다(단계 1001).

마크등록요구를 수신한 마크관리서버(101)는 마크관리처리부(221)에 의해 등록요구자의 사원ID(401)를 바탕으로 마크관리DB(210)에서 요구자의 메일주소(404)를 읽어내어, 요구자의 메일주소(404)로 마크요구/변경의 확인의뢰를 송신한다(단계 1002 및 단계 1003).

확인의뢰를 수신한 사원단말(111)의 마크등록처리부(312)는, 이미지스캐너 등을 이용하여 작성한 등록 혹은 변경하고자 하는 인영디자인을 마크의 요구확인결과와 함께 마크관리서버(101)로 송신한다(단계 1004 및 단계 1005). 스캐너 대신에 디지털카메라나 디지털콘텐트 작성소프트를 이용하여 인영 또는 서명의 디자인을 작성할 수도 있다.

인영과 마크의 요구확인결과를 수신한 마크관리서버(101)는, 마크관리처리부 (221)를 이용하여 마크관리서버(101)에서 관리하는 당해 서버의 비밀키로 본인인증정보를 암호화하고, 이것을 수신한 인영디자인에 집어넣어 마크를 작성한다.(단계 1008).

마크관리DB(210) 내의 등록 혹은 변경한 마크의 정보를 갱신한 후(단계 1009), 그 본인인증정보를 복호하기 위한 공개키와 함께 상기 작성한 마크를 요구자인 사원(110)에게 FD 등으로 배포한다(단계 1010). 사원(110)은 배포된 마크를 사원단말(111)에 격납한다(단계 1011 및 단계 1012).

도 11은 본 실시예의 마크날인처리의 처리절차를 나타내는 순서도이다. 도 11에서는 사원단말(111)에 있어서 문서인증정보를 집어넣은 마크를 문서에 날인하는 처리순서를 나타내고 있다. 도 12는 본 실시예의 도 11의 처리순서에 대응하는 처리화면의 이미지를 나타내는 도이다. 이 도 11 및 도 12와 상술한 도 9를 이용하여 상기 처리순서를 설명하기로 한다.

우선, 사원(110)이 날인하고자 하는 문서데이터 등을 기본기능 표시영역 (903)에 있는 파일버튼으로 선택하여, 디지털데

이터 표시영역(901)에 표시한다(단계 1101).

마크기능 표시영역(902)의 마크의 호출버튼을 클릭하면, 마크날인처리부 (313)에 의해 도 12의 처리화면이미지(1201)와 같은 사원ID(401)와 비밀번호의 입력란이 표시된다(단계 1102 및 단계 1103).

마크날인처리부(313)는, 입력된 비밀번호와 미리 사원단말(111)에 격납되어 있는 비밀번호를 조회하여, 합치하지 않은 경우에는 에러메세지를 표시하고, 합치한 경우에는 마크란에 마크를 표시한다(단계 1104~단계 1106).

다음으로, 문서정보를 집어넣기 위한 버튼을 클릭하면, 도 12의 처리화면이미지(1202)와 같이 마크날인처리부(313)에 의해 문서인증정보의 항목란을 표시한다(단계 1107 및 단계 1108).

필요한 항목을 선택하여 OK를 클릭하면, 마크날인처리부(313)은 선택된 문서정보와 날인통산번호를 사원마다 미리 정해져 있는 각 사원들의 고유의 비밀키로 암호화하여 마크에 집어넣고, 또한 그 복호화에 필요한 공개키를 첨부하여 마크란에 그 마크를 표시한다(단계 1109~단계 1113).

날인위치를 선택하여 마크기능 표시영역(902)의 날인버튼을 클릭하면, 마크날인처리부(313)는 마크를 문서의 설정된 위치에 날인한다(단계 1114~단계 1116). 날인한 후, 도시되어 있는 발주서를 보낼 수 있다. 단, 여기서 문서에 날인하지 않고 정보가 들어있는 마크를 단독으로 보낼 수도 있다. 또한, 문서인증정보의 복호을 위해 필요한 사원 고유의 공개키는, 마크에 첨부시키지 않고 본인인증시에 취득하는 것으로 할 수도 있다.

도 13은 본 실시예의 본인인증처리의 처리절차를 나타내는 순서도이다. 도 14는 본 실시예의 도 13의 처리순서에 대응하는 처리화면의 이미지예를 나타내는 도이다. 우선, 사원단말(111)에서 도 14의 처리화면이미지(1401)와 같이 마크가 붙어 있는 디지털데이터를 표시하고, 사원(110)이 마크의 인증버튼을 클릭하면, 마크인증처리부(314)는 마크의 인증항목란을 표시한다(단계 1301 및 단계 1302).

도 14의 처리화면이미지(1402)와 같이 사원(110)이 마크의 본인인증항목을 클릭하면, 마크인증처리부(314)는 그 마크에서 본인인증정보를 추출한다(단계 1303). 추출한 본인인증정보를 복호화하기 위한 공개키가 사원단말(111) 혹은 공개키 DB(309)에 격납되어 있는 공개키와 합치하는 지의 여부를 조회한다(단계 1305).

복호화하기 위한 공개키가 합치한 경우에는, 마크인증처리부(314)는 그 마크에서 추출한 본인인증정보를 복호화하고, 내용을 확인할 수 있도록 도 14의 처리화면이미지(1403)와 같이 본인인증정보를 표시하고(단계 1306), 합치하지 않으면 에러메세지를 표시한다(단계 1307). 또한, 에러메세지를 표시한 경우에는, 인영을 지우거나 인영에 × 표시를 하는 등 마크를 무효인 디자인으로 변형한다(단계 1308).

또한, 본인인증정보로서 표시된 내용을 본인에게 확인하고자 하는 경우에는, 본인인증정보 중의 메일주소로 확인의뢰 메일을 송신한다. 또한, 본인인증결과의 표시방법은 도 14의 처리화면이미지예에 한정되는 것이 아니라, 예를들어 에러메세지는 음성 등에 의해 표현할 수도 있다.

도 15는 본 실시예의 문서인증처리의 처리절차를 나타내는 순서도이다. 또한, 문서인증처리순서의 최초 공정에서, 본인인증처리순서와 동일한 부분, 즉 도 13에서 말하자면 단계 1301 및 단계 1302에 상당하는 부분은 생략하였다. 도 16은 본 실시예의 도 15의 처리순서에 대응하는 처리화면의 이미지예를 나타내는 도이다.

우선, 사원(110)이 사원단말(111)에서 도 16의 처리화면이미지(1601)와 같이 마크의 문서인증항목을 클릭한다(단계 1501). 마크인증처리부(314)는, 그 마크에서 문서정보의 복호화에 필요한 공개키와 문서인증정보를 추출하여 문서인증정보를 복호화한다(단계 1502~단계 1504).

다음으로, 그 마크가 날인되어 있는 문서 등의 디지털 데이터에서 특징정보를 추출하고, 그 마크에서 추출한 문서인증정보 중의 특징정보(707)와 비교조회한다(단계 1505 및 단계 1506).

그 결과, 합치하지 않은 경우에는 문서 등의 디지털데이터가 작성시점의 것과 다르게 되기 때문에, 「이 데이터는 변경되

어 있습니다」 등의 에러메세지를 표시함과 동시에 인영을 지우거나 인영에 × 표를 붙이는 등, 마크를 무효인 디자인으로 변형한다(단계 1507 및 단계 1508).

특징정보(707)가 합치한 경우에는, 유효기한 등의 정보를 확인하여 OK가 되면 도 16의 단계처리화면 이미지(1602)와 같이 확인을 위한 문서정보의 표시를 수행하고(단계 1509 및 단계 1510), 유효기한(704)이 지난 경우 등에는 인영을 지우거나 인영에 × 표를 붙이는 등, 마크를 무효인 디자인으로 변형한다(단계 1508). 또한, 문서인증결과의 표시방법은, 도 16의 처리화면이미지예에 한정되는 것이 아니라, 예를들어 에러메세지의 표시는 소리 등으로 할 수도 있다.

마크의 제 3자에 의한 부정날인을 방지하기 위해 비밀번호를 이용하고 있는데, 보다 보안성을 높이기 위해서는 예를들어 비밀번호를 ID카드로 관리하고, 사용할 때에는 마크인증처리부(314)에 의해 ID카드에서 비밀번호를 판독하도록 할 수도 있다. 이 때, 비밀번호를 미리 암호화해 두면 보다 보안성이 높아진다.

또한, 본인인증정보만이 들어있는 다른 사람의 마크를 부정하게 입수하여 자신의 비밀키로 문서정보를 그 마크에 집어넣어, 부정하게 사용하는 등에 대한 대응책으로는, 예를들어 마크의 날인통산번호(702)를 이용한다. 사원단말(111)에서 문서인증정보를 집어넣은 마크를 날인할 때에, 날인통산번호(702)를 로그이력정보로 하여 자동적으로 마크관리서버(101)로 송신하고, 마크로그관리DB(212)에서 로그정보를 관리함으로써 상술한 바와 같은 부정이 이루어졌을 때에 체크할 수 있다.

이상, 본 발명의 실시예에 대하여 기업내부 네트워크 및 기업간의 네트워크의 예를 이용하여 설명하였는데, 본 발명은 이 실시예에 한정되는 것이 아니다. 예를들면, 개인이 네트워크상에서 전자상거래를 실시할 때에 작성하는 주문서와 같은 네트워크 상에서 주고받는 일반적인 디지털데이터에 적용할 수도 있다. 또한, 종래 인감증명을 발행했던 지방자치체가 마크관리기관으로 되어 인감도장의 인감등록시에 마크를 신청한 사람에 대해서 FD 등으로 본인인증정보를 집어넣은 마크와 마크인증처리부(314)를 배포하는 방법도 생각할 수 있다. 디지털데이터는, 문서에 한정되는 것이 아니라 지도 등의 화상데이터나 동화(動畵)데이터로 할 수도 있다.

또한, 출석이나 투표를 위한 서명데이터가 들어있는 마크를 관리자단말이나 데이터베이스로 송신할 수도 있다.

발명의 효과

이상, 설명한 바와 같이 본 실시예의 전자마크 인증시스템에 의하면, 본인인증정보 및 디지털데이터 인증정보를 집어넣어 작성한 마크를 디지털데이터에 부가하고, 마크내의 인증정보를 이용하여 당해 디지털데이터의 인증을 수행하기 때문에, 네트워크상에서 디지털데이터를 송수신할 때의 본인인증 및 데이터인증을 실현할 수 있다.

(57) 청구의 범위

청구항 1. 디지털마크에 의해 데이터를 인증하기 위한 마크를 제공하기 위한 디지털마크 인증시스템으로서,

마크를 작성하기 위한 요구에 따라서, 디스플레이상에서 시인성(視認性)이 있는 마크를 작성하기 위해 요구자의 마크디자인에 요구자의 인증정보를 집어넣는 마크관리처리부(221)와,

상기 마크를 복호(復號)화하기 위한 복호(復號)키(key)와 상기 시인성마크를 요구자 단말장치에 배포하는 마크배포부(200-222)를 가지는 것을 특징으로 하는 디지털마크 인증시스템.

청구항 2. 청구항 1에 있어서,

상기 복호키를 기억하는 복호키관리 데이터베이스와,

상기 복호키를 상기 마크관리서버에 접속된 복수의 마크단말장치에 송신하는 복호키처리부(222)를 가지는 것을 특징으로 하는 디지털마크 인증시스템.

청구항 3. 청구항 1에 있어서,

상기 작성된 마크 중에 상기 인증정보가 들어있다고 하는 것이 디스플레이상에서 눈으로 직접 확인할 수 있는 것을 특징으로 하는 디지털마크 인증시스템.

청구항 4. 청구항 1에 있어서,

상기 인증정보는,

요구자의 특징을 포함하는 정보를 암호키로 암호화함으로써 얻을 수 있는 것을 특징으로 하는 디지털마크 인증시스템.

청구항 5. 청구항 1에 있어서,

마크를 갱신하기 위한 요구에 따라서, 상기 마크관리처리부(221)는,

요구자의 다른 인증정보를 작성하기 위하여 요구자의 다른 특징으로 포함하는 정보를 암호키로 암호화하고, 상기 마크를 작성하기 위하여 요구자의 마크디자인에 상기 다른 인증정보를 집어넣는 것을 특징으로 하는 디지털마크 인증시스템.

청구항 6. 청구항 1에 있어서,

상기 마크를 작성하기 위한 요구에 따라서, 마크관리처리부(221)는,

요구자의 인증정보를 작성하기 위하여 요구자의 다른 특징을 포함하여 작성되는 상기 마크안에 다른 인증정보가 들어있다는 것을 디스플레이상에서 눈으로 직접 확인할 수 없는 상기 다른 인증정보를 마크디자인에 집어넣는 것을 특징으로 하는 디지털마크 인증시스템.

청구항 7. 청구항 6에 있어서,

상기 인증정보와 상기 다른 인증정보는,

상기 마크안의 분할된 다른 장소에 집어넣는 것을 특징으로 하는 디지털마크 인증시스템.

청구항 8. 디지털마크에 의해 데이터를 인증하기 위한 마크를 디지털데이터에 부가하는 단말장치로서,

마크를 작성하기 위한 요구를 디지털마크 인증시스템에 송신하고, 그 시스템으로부터 요구자 본인의 특징을 포함하는 정보를 암호키로 암호화하여 요구자의 마크디자인에 상기 인증정보를 집어넣은 마크를 수신하여 기억하는 마크처리부(312)와,

상기 마크를 복호화하기 위한 복호키를 수신하여 격납하기 위한 복호키 데이터베이스(315)와,

송신될 디지털데이터를 인증하기 위하여 상기 디지털데이터의 로그정보를 상기 암호키로 암호화하여 상기 마크에 집어넣어 상기 디지털데이터와 함께 송신하는 송신부(303)를 가지는 것을 특징으로 하는 단말장치.

청구항 9. 적어도 하나의 클라이언트단말과 상기 클라이언트단말에서 사용되는 마크를 관리하는 적어도 하나의 관리서버가 통신망을 매개로 상호 접속되어 있으며,

상기 마크관리서버는,

상기 클라이언트단말로부터 마크의 등록 혹은 변경요구를 받은 경우에, 디지털데이터의 작성자의 본인인증을 수행하기 위하여 필요한 정보를 마크에 집어넣어 상기 클라이언트단말에 송부하는 수단을 갖추며,

상기 클라이언트단말은,

디지털데이터의 문서인증을 수행하기 위하여 필요한 정보를 마크에 집어넣는 수단과,

디지털데이터의 본인인증 및 문서인증의 어느 한 쪽 또는 양쪽을 모두 수행하는 수단을 갖춘 것을 특징으로 하는 전자인감 인증시스템.

청구항 10. 청구항 9에 있어서,

마크발행시에 본인인증을 위하여 필요한 정보를 하나의 화상이미지데이터 내의 하나의 블럭에 부여하고,

문서송신시에 문서인증을 위해 필요한 정보를 다른 블럭에 부여하여 본인인증 및 문서인증의 어느 한쪽 또는 양쪽 모두를 수행하는 수단을 갖춘 시인성이 있는 인감마크를 생성하는 것을 특징으로 하는 전자인감 인증시스템.

청구항 11. 디지털마크에 의해 데이터를 인증하기 위한 마크를 제공하기 위한 디지털마크 인증방법으로서,

마크를 작성하기 위한 요구에 따라서, 디스플레이상에서 시인성이 있는 마크를 작성하기 위하여 요구자의 마크디자인에 요구자의 인증정보를 집어넣는 단계(1008)와,

상기 마크를 복호화하기 위한 복호키와 상기 시인성마크를 요구자 단말장치에 배포하는 단계(1010)를 가지는 것을 특징으로 하는 디지털마크 인증방법.

청구항 12. 청구항 11에 있어서,

상기 복호키를 기억하는 복호키관리 데이터베이스에서 상기 복호키를 상기 마크관리서버에 접속된 복수의 마크단말장치로 송신하는 단계(1010)를 가지는 것을 특징으로 하는 디지털마크 인증방법.

청구항 13. 청구항 11에 있어서,

상기 작성된 마크안에 상기 인증정보가 들어있다는 것이 디스플레이상에서 눈으로 직접 확인할 수 있는 것을 특징으로 하는 디지털마크 인증방법.

청구항 14. 청구항 11에 있어서,

상기 인증정보를 얻기 위하여, 요구자의 특징을 포함하는 정보를 암호키로 암호화하는 단계를 가지는 것을 특징으로 하는 디지털마크 인증방법.

청구항 15. 청구항 11에 있어서,

마크를 갱신하기 위한 요구에 따라서, 요구자의 다른 인증정보를 작성하기 위하여 요구자의 다른 특징을 포함하는 정보를 암호키로 암호화하고, 상기 마크를 작성하기 위하여 요구자의 마크디자인에 상기 다른 인증정보를 집어넣는 단계를 가지는 것을 특징으로 하는 디지털마크 인증방법.

청구항 16. 청구항 11에 있어서,

상기 마크를 작성하기 위한 요구에 따라서, 요구자의 인증정보를 작성하기 위하여 요구자의 다른 특징을 포함하여 작성되는 상기 마크안에 다른 인증정보가 들어있다는 것을 디스플레이상에서 눈으로 직접 확인할 수 없는 상기 다른 인증정보를 마크디자인에 집어넣는 단계를 가지는 것을 특징으로 하는 디지털마크 인증방법.

청구항 17. 청구항 16에 있어서,

상기 인증정보와 상기 다른 인증정보를 상기 마크안의 분할된 다른 장소에 집어넣는 것을 특징으로 하는 디지털마크 인증방법.

청구항 18. 디지털마크에 의해 데이터를 인증하기 위한 마크를 디지털데이터에 부가하는 단말장치를 운전하는 방법으로서,

마크를 작성하기 위한 요구를 디지털마크 인증시스템에 송신하고, 그 시스템으로부터 요구자 본인의 특징을 포함하는 정보를 암호키로 암호화하여 요구자의 마크디자인에 상기 인증정보를 집어넣은 마크를 수신하여 기억하는 단계(1011)와,

상기 마크를 복호화하기 위한 복호키를 수신하여 격납하는 단계(1012)와,

송신될 디지털데이터를 인증하기 위하여 상기 디지털데이터의 로그정보를 상기 암호키로 암호화하여 상기 마크에 집어넣어 상기 디지털데이터와 함께 송신하는 단계(1116)를 가지는 것을 특징으로 하는 단말장치 운전방법.

청구항 19. 디지털마크에 의해 데이터를 인증하기 위한 마크를 제공하기 위한 디지털마크 인증방법으로서,

마크를 작성하기 위한 요구에 따라서 디스플레이상에서 시인성이 있는 마크를 작성하기 위하여 요구자의 마크디자인에 요구자의 인증정보를 집어넣는 단계(1008)와,

상기 마크를 복호화하기 위한 복호키와 상기 시인성마크를 요구자 단말장치에 배포하는 단계(1010)를 가지는 것을 특징으로 하는 디지털마크 인증방법.

청구항 20. 디지털마크에 의해 데이터를 인증하기 위한 마크를 디지털데이터에 부가하는 방법으로서,

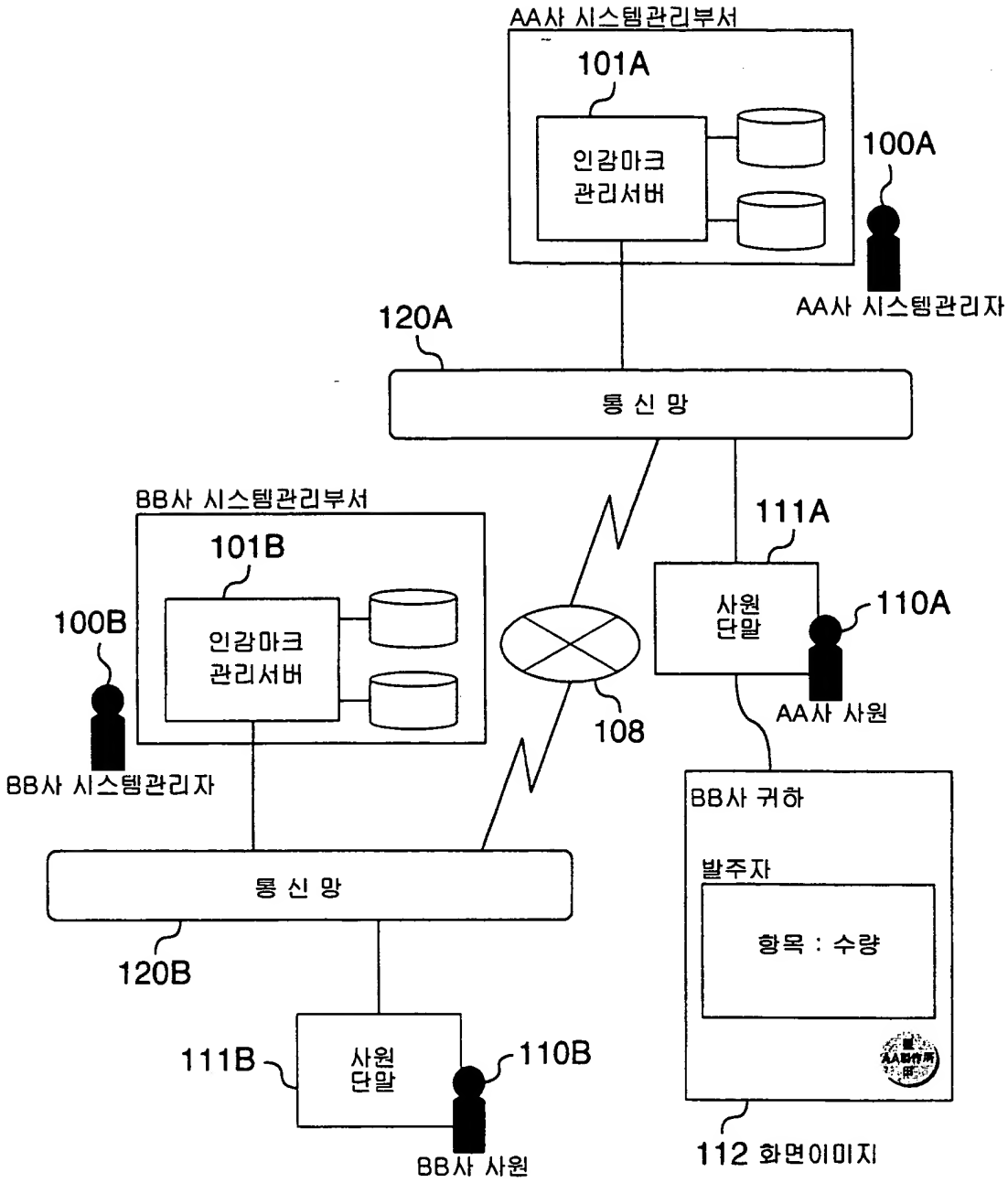
마크를 작성하기 위한 요구를 디지털마크 인증시스템에 송신하고, 그 시스템으로부터 요구자 본인의 특징을 포함하는 정보를 암호키로 암호화하여 요구자의 마크디자인에 상기 인증정보를 집어넣은 마크를 수신하여 기억하는 단계(1011)와,

상기 마크를 복호화하기 위한 복호키를 수신하여 격납하는 단계(1012)와,

송신될 디지털데이터를 인증하기 위하여 상기 디지털데이터의 로그정보를 상기 암호키로 암호화하여 상기 마크에 집어넣어 상기 디지털데이터와 함께 송신하는 단계(1116)를 가지는 것을 특징으로 하는 마크를 디지털데이터에 부가하는 방법.

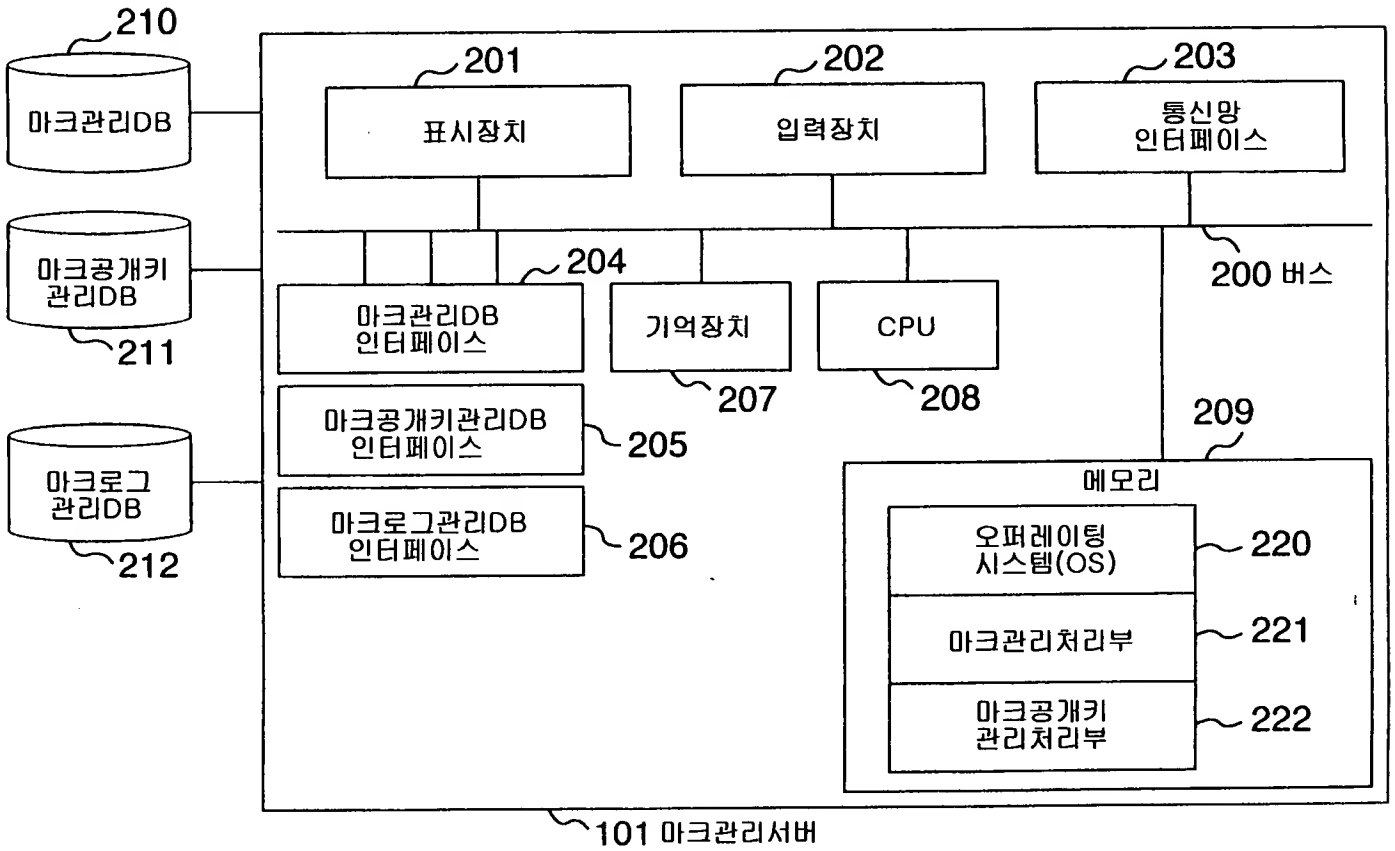
도면

도면1

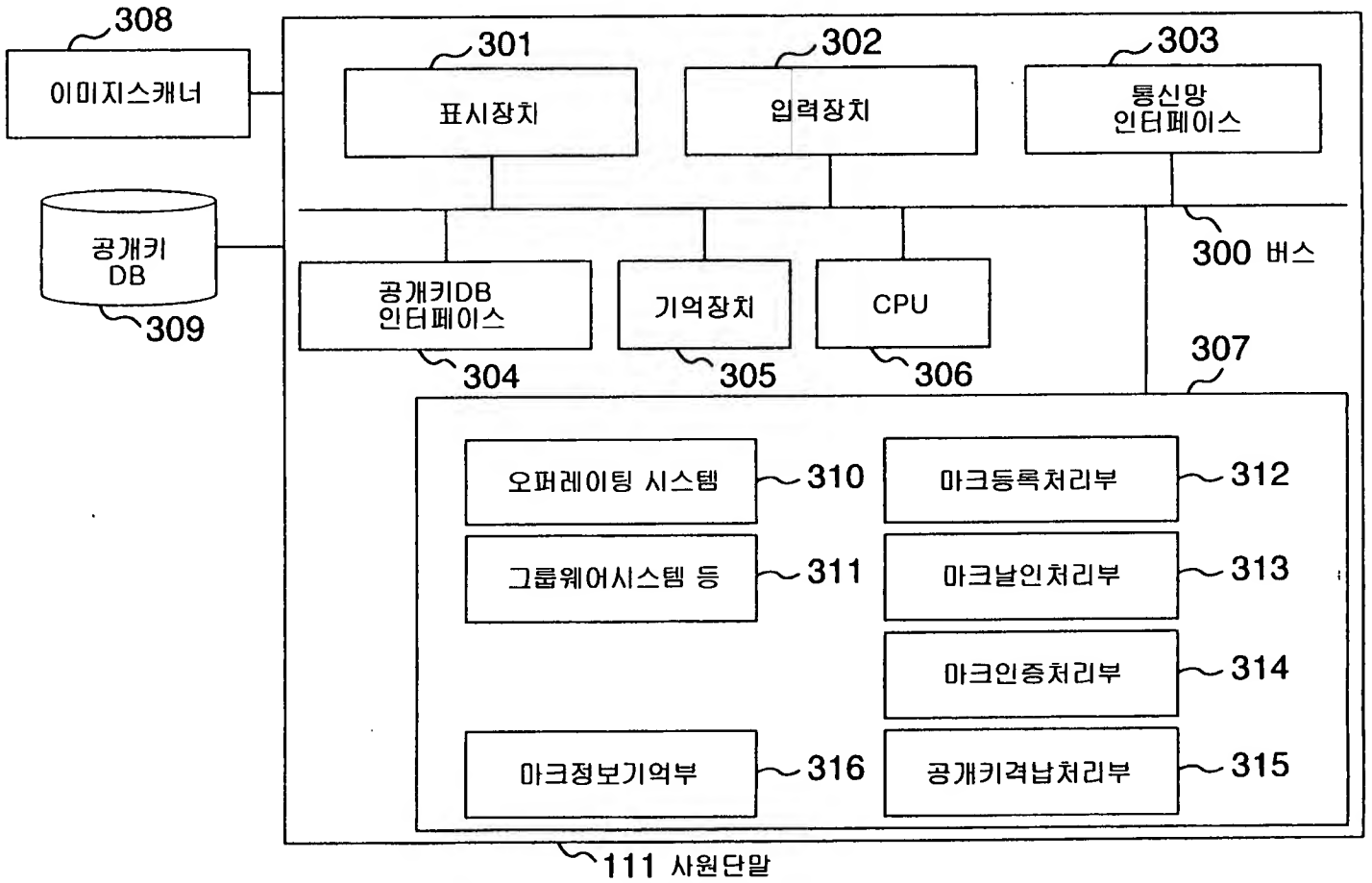

AA사 시스템관리부서
101A
인감마크
관리서버
100A
AA사 시스템관리자
120A
통 신 망
BB사 시스템관리부서
101B
100B
인감마크
관리서버
BB사 시스템관리자
111A
사원
단말
110A
AA사 사원
108
BB사 귀하
발주자
항목 : 수량
통 신 망
120B
111B
사원
단말
110B
BB사 사원
112 화면이미지

도면2

도면3


210
마크관리DB
201
표시장치
202
입력장치
203
통신망
인터페이스
마크공개키
관리DB
211
204
마크관리DB
인터페이스
기억장치
207
CPU
208
200 버스
마크공개키관리DB
인터페이스
205
209
메모리
마크로그
관리DB
212
마크로그관리DB
인터페이스
206
오퍼레이팅
시스템(OS)
220
마크관리처리부
221
마크공개키
관리처리부
222
101 마크관리서버

도면4


308
이미지스캐너
301
표시장치
302
입력장치
303
통신망
인터페이스
공개키
DB
309
300 버스
공개키DB
인터페이스
304
기억장치
305
CPU
306
307
오퍼레이팅 시스템
310
마크등록처리부
312
그룹웨어시스템 등
311
마크날인처리부
313
마크인증처리부
314
마크정보기억부
316
공개키격납처리부
315
111 사원단말

도면5

401 사원ID	402 인감ID	403 성 명	404 메일주소	405 소속 . 직책외	406 인 영
D001101117	A00123	아이카와타로우	Aikawa@aa.co.jp	OO사업부 사업부장	
A035410506	A00124	아이다지로우	Aida@aa.co.jp	OO사업부 과장	
H001100402	–	아이노산로우	Aino@aa.co.jp	OO사업부 담당	–

501	502	503	504
NO.	인감마크관리자	관리자주소	공개키
1	A사인감마크관리	im@aa.co.jp	pw****gl*****qqm*
2	B사인감마크관리	im@bb.co.jp	*ajk**yu*****aqz*r

도면6

601	602	603	604
인감ID	성명	메일주소	소속 · 직책외
A00123	아이카와타로우	Aikawa@aa.co.jp	OO사업부 사업부장

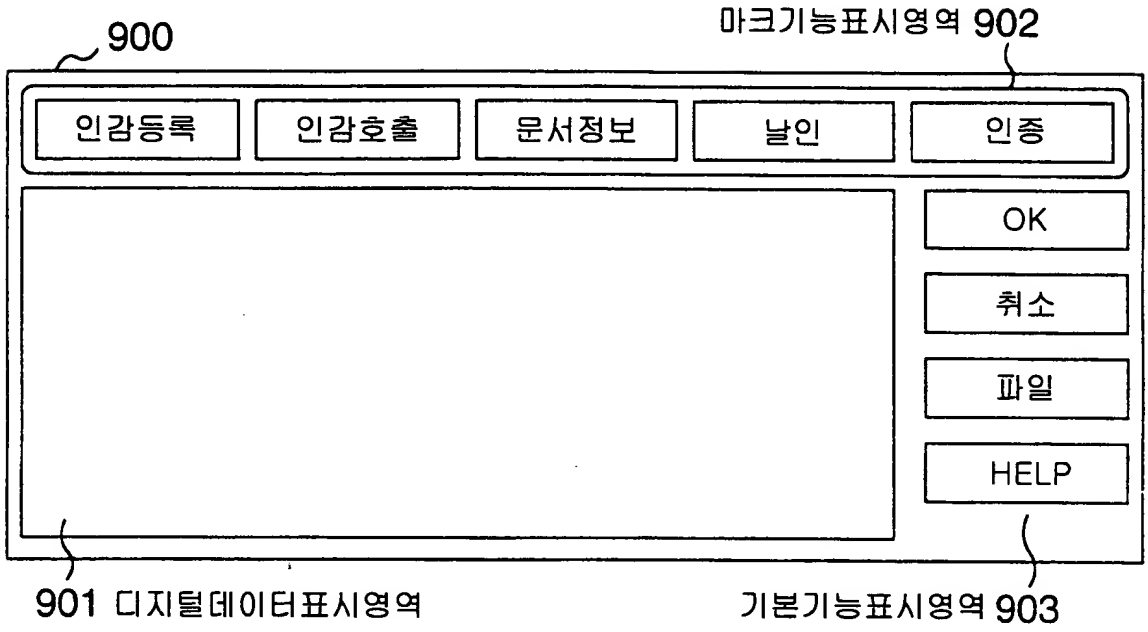
도면7

701	702	703	704	705	706	707
인감ID	통신No.	작성일자	유효기한	파일명	단말ID	데이터의 특징정보
A00123	000089	1998.7.7	1998.12.31	158.2**/**.doc	PC792	********

도면8

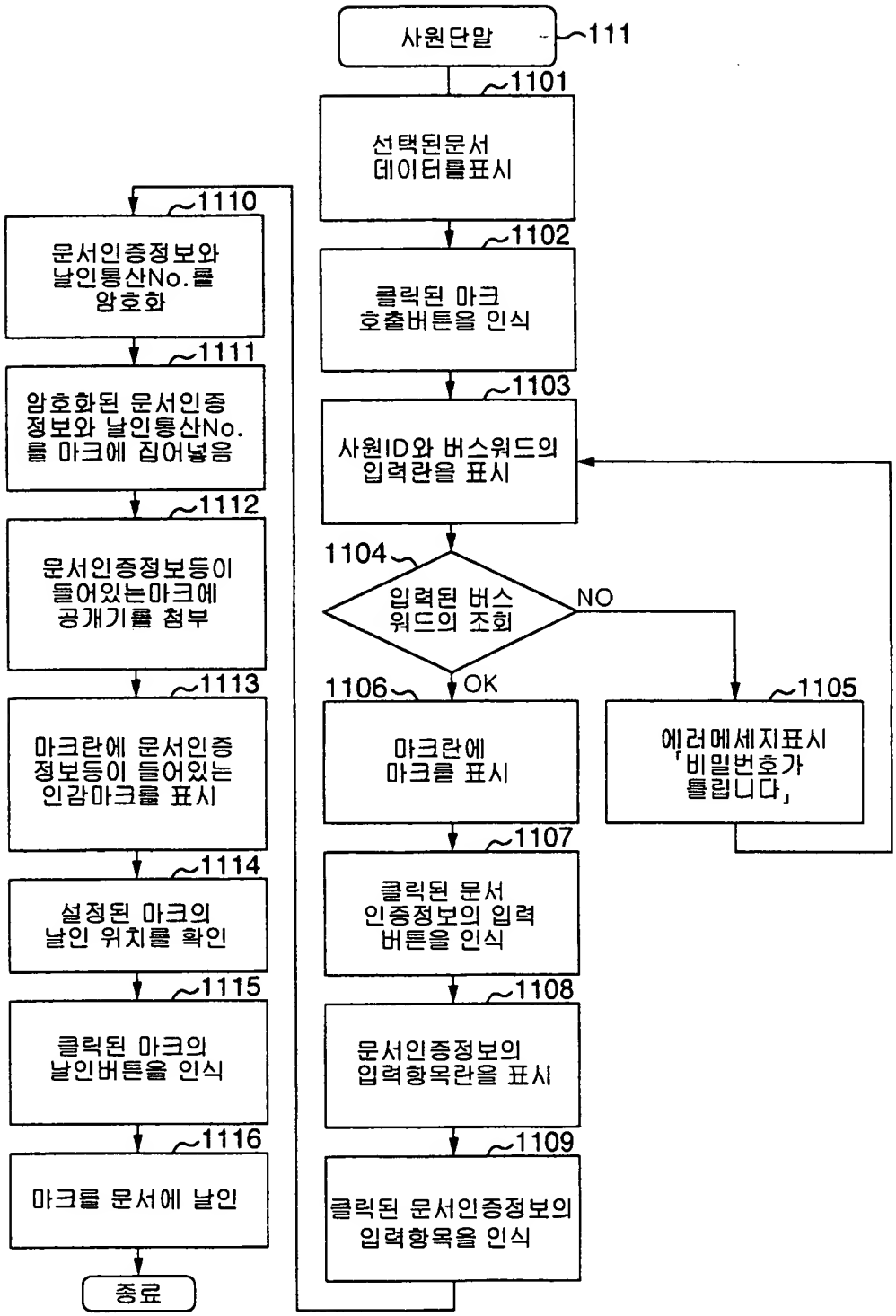

藍
田
801
藍
AA제작소
田
802
藍
AA제작소
田
803

도면9

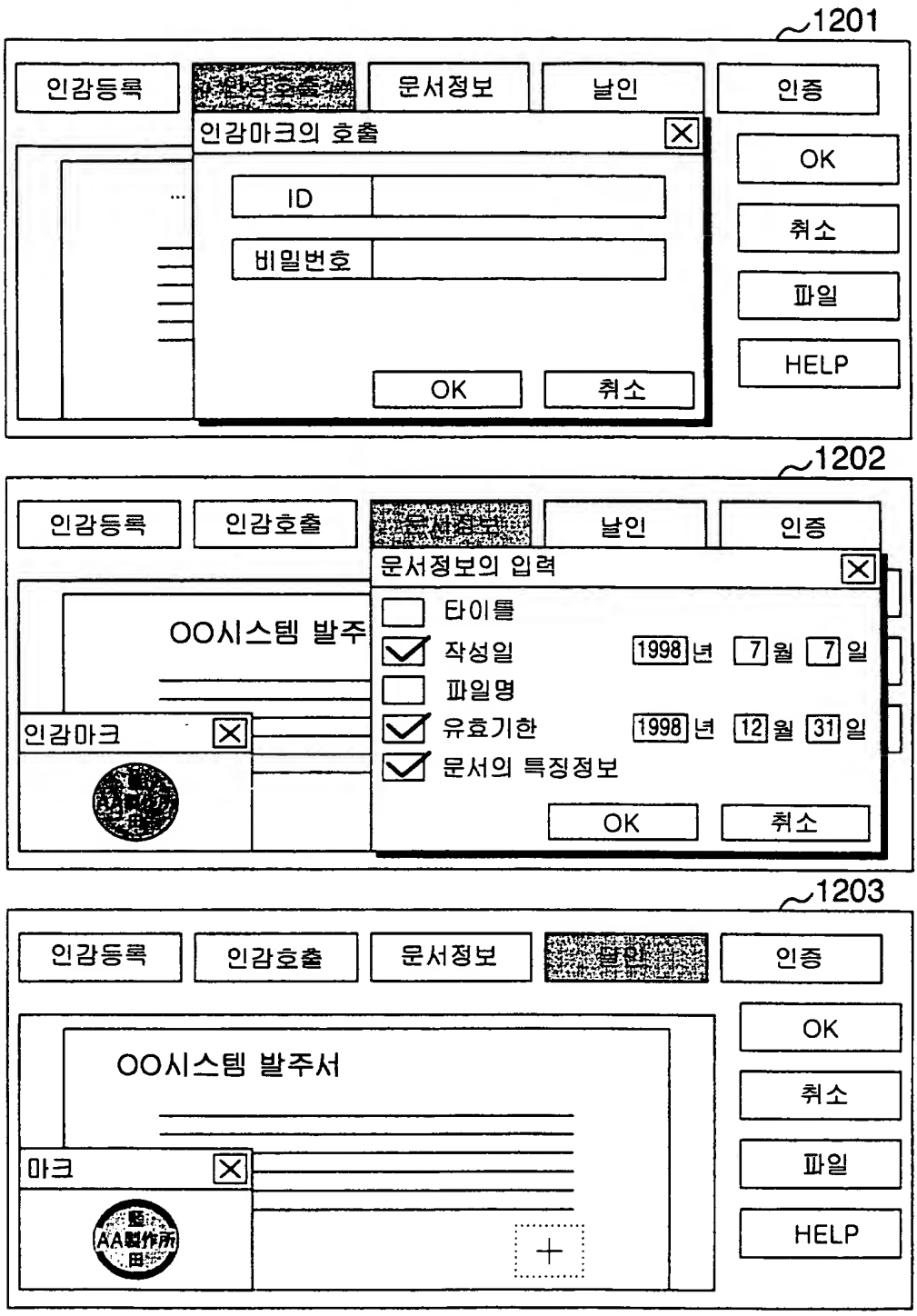

900
마크기능표시영역 902
인감등록
인감호출
문서정보
날인
인증
OK
취소
파일
HELP
901 디지털데이터표시영역
기본기능표시영역 903

도면10

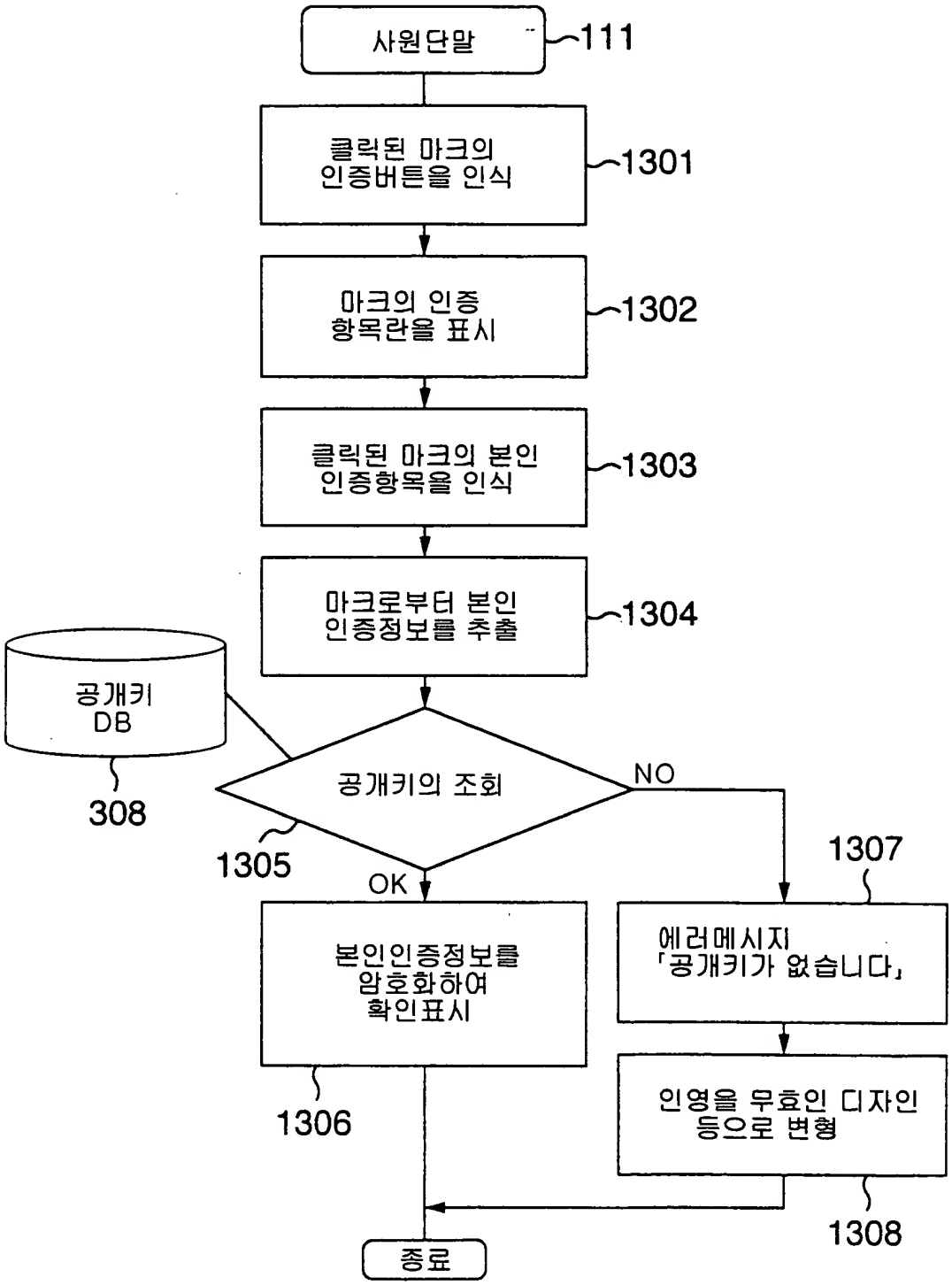
도면11


사원단말
111
1101
선택된문서 데이터를표시
1102
클릭된 마크 호출버튼을 인식
1103
사원ID와 버스워드의 입력란을 표시
1104
입력된 버스 워드의 조회
NO
OK
1105
에러메세지표시 「비밀번호가 틀립니다」
1106
마크란에 마크를 표시
1107
클릭된 문서 인증정보의 입력 버튼을 인식
1108
문서인증정보의 입력항목란을 표시
1109
클릭된 문서인증정보의 입력항목을 인식
1110
문서인증정보와 날인통산No.를 암호화
1111
암호화된 문서인증 정보와 날인통산No. 를 마크에 집어넣음
1112
문서인증정보등이 들어있는마크에 공개기를 첨부
1113
마크란에 문서인증 정보등이 들어있는 인감마크를 표시
1114
설정된 마크의 날인 위치를 확인
1115
클릭된 마크의 날인버튼을 인식
1116
마크를 문서에 날인
종료

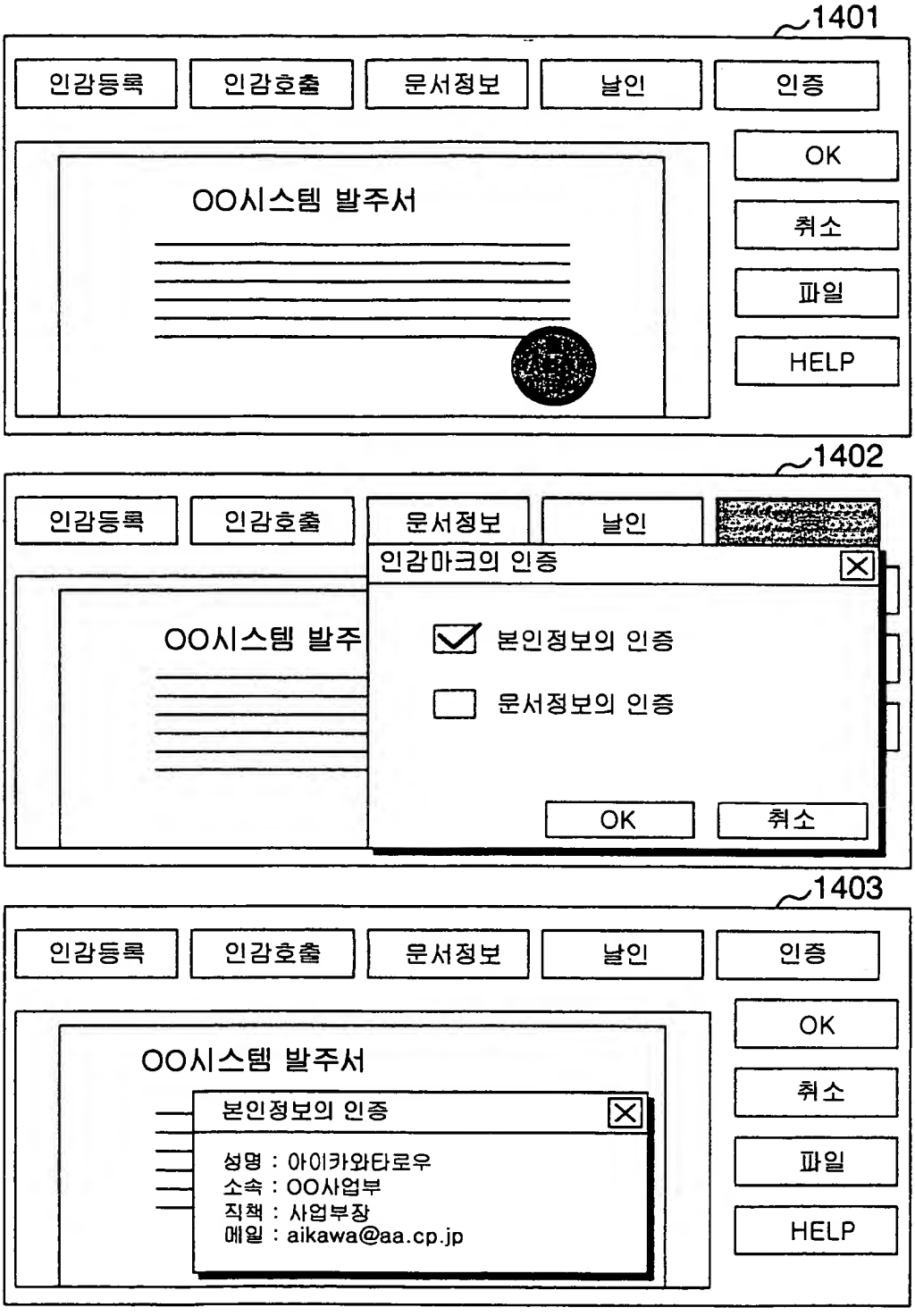
도면12


1201
인감등록
인감호출
문서정보
날인
인증
인감마크의 호출
ID
비밀번호
OK
취소
OK
취소
파일
HELP
1202
인감등록
인감호출
문서정보
날인
인증
문서정보의 입력
OO시스템 발주
타이틀
작성일
1998 년 7 월 7 일
파일명
유효기한
1998 년 12 월 31 일
문서의 특징정보
인감마크
OK
취소
1203
인감등록
인감호출
문서정보
날인
인증
OO시스템 발주서
마크
OK
취소
파일
HELP

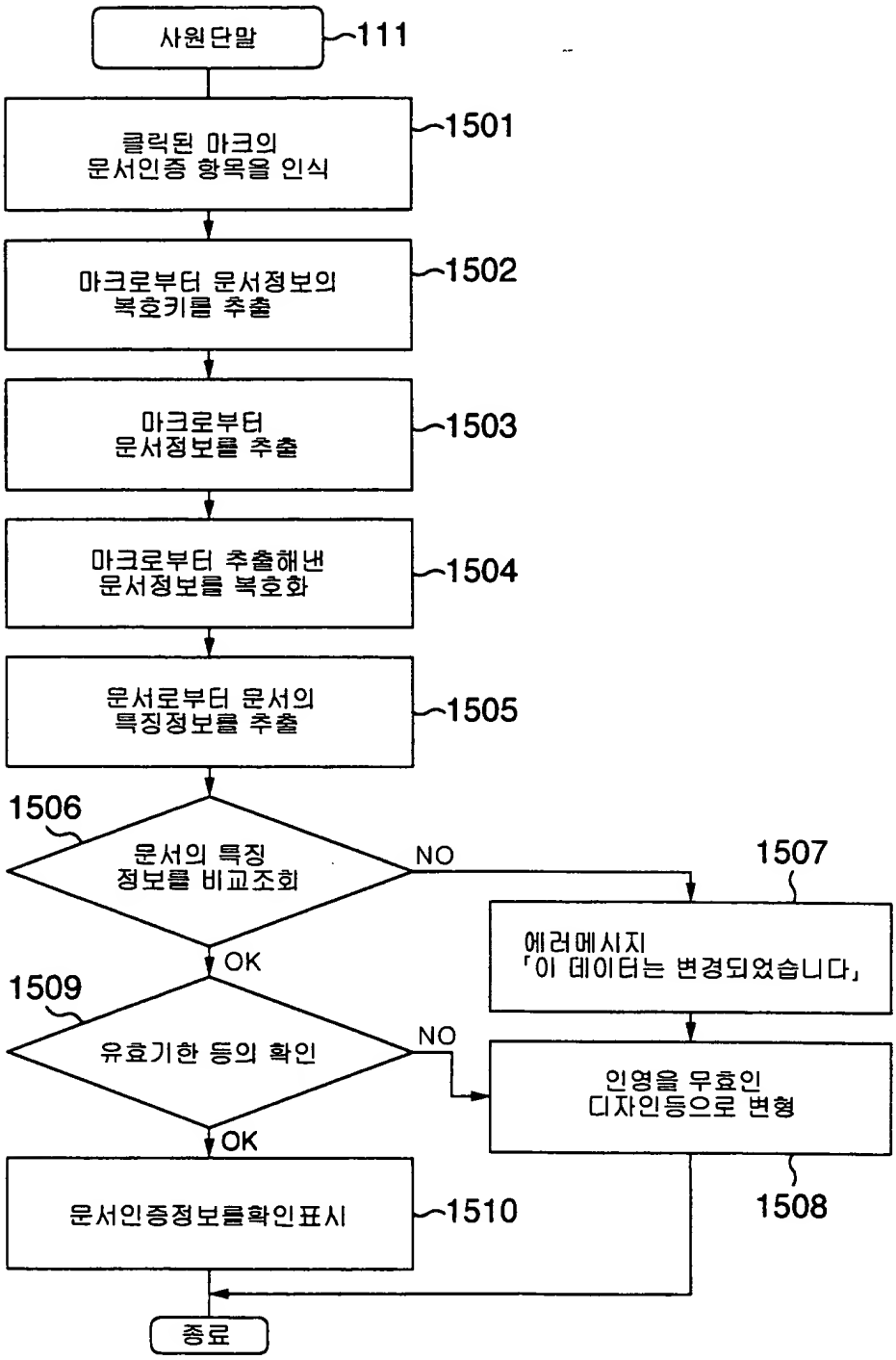
도면13


사원단말
111
클릭된 마크의
인증버튼을 인식
1301
마크의 인증
항목란을 표시
1302
클릭된 마크의 본인
인증항목을 인식
1303
마크로부터 본인
인증정보를 추출
1304
공개키
DB
308
공개키의 조회
1305
NO
OK
1307
본인인증정보를
암호화하여
확인표시
1306
에러메시지
「공개키가 없습니다」
인영을 무효인 디자인
등으로 변형
1308
종료

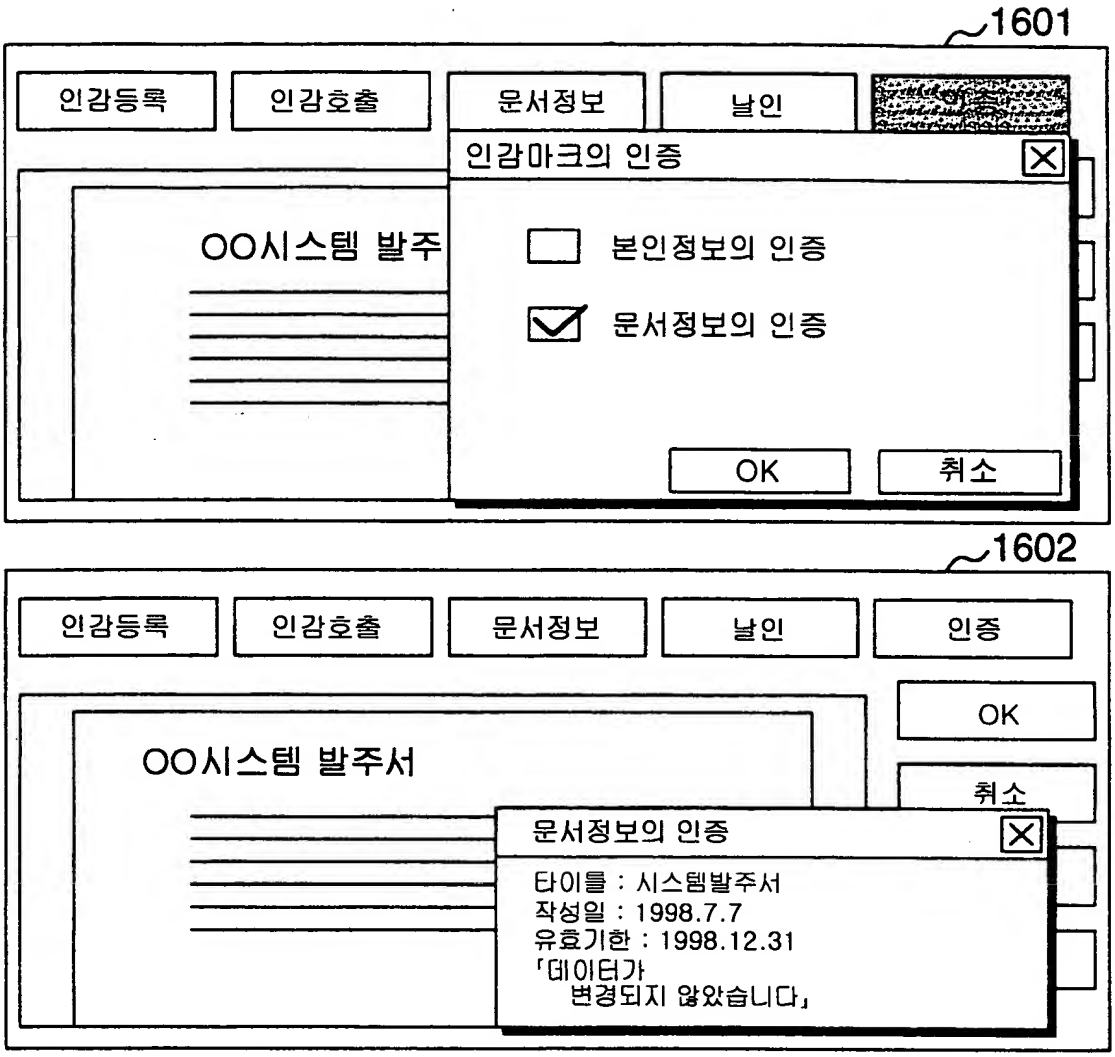
도면14


1401
인감등록
인감호출
문서정보
날인
인증
OO시스템 발주서
OK
취소
파일
HELP
1402
인감등록
인감호출
문서정보
날인
인감마크의 인증
OO시스템 발주
본인정보의 인증
문서정보의 인증
OK
취소
1403
인감등록
인감호출
문서정보
날인
인증
OO시스템 발주서
본인정보의 인증
성명 : 아이카와타로우
소속 : OO사업부
직책 : 사업부장
메일 : aikawa@aa.cp.jp
OK
취소
파일
HELP

도면15


사원단말
111
클릭된 마크의
문서인증 항목을 인식
1501
마크로부터 문서정보의
복호키를 추출
1502
마크로부터
문서정보를 추출
1503
마크로부터 추출해낸
문서정보를 복호화
1504
문서로부터 문서의
특징정보를 추출
1505
1506
문서의 특징
정보를 비교조회
NO
1507
에러메시지
「이 데이터는 변경되었습니다」
OK
1509
유효기한 등의 확인
NO
인영을 무효인
디자인등으로 변형
OK
문서인증정보를확인표시
1510
1508
종료

도면16


1601
인감등록
인감호출
문서정보
날인
인감마크의 인증
OO시스템 발주
본인정보의 인증
문서정보의 인증
OK
취소
1602
인감등록
인감호출
문서정보
날인
인증
OK
취소
OO시스템 발주서
문서정보의 인증
타이틀 : 시스템발주서
작성일 : 1998.7.7
유효기한 : 1998.12.31
「데이터가
변경되지 않았습니다」